Unisenac
Centro Universitário RS

Senac Fecomércio Sesc

Computação em Nuvem

CURSO SUPERIOR DE TECNOLOGIA EM ANÁLISE E DESENVOLVIMENTO DE SISTEMAS
CURSO SUPERIOR DE TECNOLOGIA EM REDES DE COMPUTADORES

Prof. Guto Muniz

Modelo de responsabilidade compartilhada da AWS

- **Definição:** A segurança na AWS é uma responsabilidade compartilhada entre a AWS e o cliente.

- **Objetivo:** Reduzir a carga operacional do cliente, enquanto oferece flexibilidade e controle na implantação de soluções.

- **Divisão:** A AWS cuida da segurança da infraestrutura, enquanto o cliente é responsável pela segurança de seus dados e configurações.

Cinco grandes perspectivas usadas

- Governança & Compliance
- Implementação Técnica
- Gestão de Risco
- Aspectos Legais & Contratuais
- Educação & Treinamento

Segurança *"da"* Nuvem vs. Segurança *"na"* Nuvem

- **Segurança *"da"* Nuvem:** Responsabilidade da AWS pela proteção de:
- Infraestrutura física (data centers)
- Hardware, software, redes e virtualização que suportam os serviços na nuvem.

- **Segurança *"na"* Nuvem:** Responsabilidade do cliente pela proteção de:
- Dados em repouso e em trânsito (criptografia)
- Configuração da rede (grupos de segurança, firewalls)
- Gerenciamento de identidade e acesso (IAM)
- Atualizações e patches de segurança do sistema operacional.

Segurança *"da"* Nuvem

- **A AWS é responsável pela segurança da infraestrutura.**

- **Inclui:**
  - Camada de virtualização.
  - Segurança física das instalações.
  - Gerenciamento de hardware, software e redes.

Segurança *"na"* Nuvem

- **O cliente é responsável pela segurança de seus dados e aplicações.**

- **Inclui:**
  - Criptografia de dados em repouso e em trânsito.
  - Configuração da rede para segurança.
  - Gerenciamento de credenciais e logins.
  - Grupos de segurança e atualizações de sistema operacional.

Segurança Operada pela AWS

- Proteção da infraestrutura global.
- Monitoramento contínuo de ameaças.
- Certificações de segurança como ISO 27001, SOC 1, 2, 3.
- Controles rígidos de acesso físico e virtual.

O Que o Cliente Deve Fazer?

- Gerenciar suas credenciais e permissões (IAM).
- Garantir a configuração correta de firewalls e grupos de segurança.
- Configurar a criptografia para proteger os dados.
- Manter o sistema operacional atualizado com patches de segurança.

O Que o Cliente Deve Fazer?

- **Gerenciar credenciais e permissões (IAM)**
  - Criar usuários, grupos e funções com o princípio do menor privilégio.
  - Rodar auditorias periódicas em políticas e rotacionar chaves de acesso.

- **Configurar corretamente firewalls e grupos de segurança**
  - Definir regras de entrada e saída nos Security Groups.
  - Usar Network ACLs para controle adicional em sub-redes.

O Que o Cliente Deve Fazer?

- **Gerenciar credenciais e permissões (IAM)**
  - Criar usuários, grupos e funções com o princípio do menor privilégio.
  - Rodar auditorias periódicas em políticas e rotacionar chaves de acesso.

- **Configurar corretamente firewalls e grupos de segurança**
  - Definir regras de entrada e saída nos Security Groups.
  - Usar Network ACLs para controle adicional em sub-redes.

O Que o Cliente Deve Fazer?

- **Configurar criptografia para proteger os dados**
  - Ativar criptografia em repouso (S3, EBS, RDS) e em trânsito (TLS).
  - Gerenciar chaves no AWS KMS, aplicando políticas de rotação.

- **Manter o sistema operacional atualizado com patches de segurança**
  - Automatizar updates regulares de kernels e pacotes do guest OS nas instâncias EC2.
  - Utilizar AWS Systems Manager Patch Manager para orquestrar correções.

Modelo de responsabilidade compartilhada da AWS

Responsabilidade da AWS: segurança da nuvem

- **Responsabilidades da AWS:**
  - Segurança física dos datacenters
  - Acesso controlado e baseado em necessidades

- **Infraestrutura de hardware e software**
  - Desativação de armazenamento, registro em log de acesso ao sistema operacional (SO) do host e auditoria
- **Infraestrutura de rede**
  - Detecção de intrusão

- **Infraestrutura de virtualização**
  - Isolamento de instância

Responsabilidade da AWS: segurança da nuvem

Segurança "na" Nuvem – Responsabilidade do Cliente

- **Responsabilidade do Cliente:**
  - O cliente é responsável pela segurança de tudo o que coloca na nuvem.
  - Deve proteger o conteúdo, aplicativos, e as configurações do sistema utilizados com a AWS.

Segurança "na" Nuvem – Responsabilidade do Cliente

- **Responsabilidades Específicas do Cliente:**
  - **Sistemas Operacionais:** Seleção e proteção dos sistemas operacionais de instância.
  - **Aplicativos e Recursos AWS:** Proteção dos aplicativos que executam nos recursos da AWS.
  - **Configurações de Segurança:** Grupos de segurança, firewall e configurações de rede.
  - **Gerenciamento de Contas:** Gerenciamento seguro de contas e acessos.

- **Controle de Conteúdo:**
  - **Decisões de Segurança:** O cliente define como armazenar, acessar e proteger seus dados.
  - **Localização e Estrutura dos Dados:** O cliente escolhe em que país armazenar os dados e se eles são mascarados ou criptografados.
  - **Gerenciamento de Acesso:** Controle total sobre quem tem acesso aos dados e como esses acessos são geridos e revogados.

Segurança "na" Nuvem – Responsabilidade do Cliente

- **Responsabilidades do cliente:**
  - Sistema operacional da instância do Amazon Elastic Compute Cloud (Amazon EC2)
  - Incluindo aplicação de patches, manutenção
- **Aplicações**
  - Senhas, acesso baseado em função etc.
- Configuração do **grupo de segurança**
- **Firewalls** baseados em host ou SO
  - Incluindo sistemas de prevenção ou detecção de intrusão
- Configurações **de rede**
- Gerenciamento **de contas**
  - Configurações de permissão e login para cada usuário

Segurança "na" Nuvem – Responsabilidade do Cliente

Serviços Gerenciados pelo Cliente

- **Amazon EC2 (Elastic Compute Cloud):**
  - **Função:** Serviço que fornece capacidade de computação redimensionável na nuvem. O cliente pode configurar e gerenciar suas próprias instâncias de servidores virtuais.
  - **Responsabilidade do Cliente:** Gerenciar o sistema operacional, aplicativos, patches, segurança e escalabilidade.
  -
- **Amazon Elastic Block Store (Amazon EBS):**
  - **Função:** Armazenamento de blocos persistente para instâncias do Amazon EC2. É como um "disco rígido" virtual para suas máquinas EC2.
  - **Responsabilidade do Cliente:** Gerenciar backups, segurança dos dados armazenados e configuração de volume.
  -
- **Amazon Virtual Private Cloud (Amazon VPC):**
  - **Função:** Serviço que permite provisionar uma rede isolada logicamente na nuvem. O cliente pode definir suas próprias sub-redes, tabelas de roteamento e gateways.
  - **Responsabilidade do Cliente:** Configurar e gerenciar as redes, firewalls, roteamento e segurança da rede.

Serviços Gerenciados pela AWS

- **AWS Lambda:**
  - **Função:** Serviço de computação serverless que executa código em resposta a eventos. O cliente envia o código, e a AWS gerencia a infraestrutura necessária para executar esse código.
  - **Responsabilidade da AWS:** Gerenciar a infraestrutura, balanceamento de carga, escalabilidade e execução do código.

- **Amazon Relational Database Service (Amazon RDS):**
  - **Função:** Serviço gerenciado de banco de dados relacional. A AWS gerencia tarefas administrativas como backups, atualizações e escalabilidade.
  - **Responsabilidade da AWS:** Garantir alta disponibilidade, backup automatizado, patches de segurança e escalabilidade de banco de dados.

- **AWS Elastic Beanstalk:**
  - **Função:** Serviço que facilita o provisionamento de infraestrutura, configurando automaticamente a infraestrutura necessária para a execução de aplicativos web e serviços.
  - **Responsabilidade da AWS:** Gerenciar o ambiente de aplicação, infraestrutura subjacente, atualizações de sistema e balanceamento de carga.

Características do serviço e responsabilidade de segurança

Serviços de exemplo gerenciados pelo cliente

Amazon EC2

Amazon Elastic Block Store (Amazon EBS)

Amazon Virtual Private Cloud (Amazon VPC)

Serviços de exemplo gerenciados pela AWS

AWS Lambda

Amazon Relational Database Service (Amazon RDS)

AWS Elastic Beanstalk

Infraestrutura como um serviço (IaaS)

- O cliente tem mais flexibilidade em relação à configuração de rede e armazenamento
- O cliente é responsável por gerenciar mais aspectos da segurança
- O cliente configura os controles de acesso

Plataforma como serviço (PaaS)

- O cliente não precisa gerenciar a infraestrutura subjacente
- A AWS gerencia o sistema operacional, a aplicação de patches de banco de dados, a configuração de firewall e a recuperação de desastres
- O cliente pode se concentrar no gerenciamento de código ou dados

Infraestrutura como Serviço (IaaS) na AWS

- **Amazon EC2 (Elastic Compute Cloud):**
  - Serviço que permite executar instâncias virtuais (servidores) com diferentes sistemas operacionais, gerenciando diretamente a infraestrutura.

- **Amazon S3 (Simple Storage Service):**
  - Armazenamento de objetos escalável e seguro, usado para armazenar e recuperar dados a qualquer momento e em qualquer lugar.

- **Amazon EBS (Elastic Block Store):**
  - Serviço de armazenamento em blocos para uso com instâncias do Amazon EC2, semelhante a um disco rígido tradicional.

Plataforma como Serviço (PaaS) na AWS

- **AWS Elastic Beanstalk:**
  - Serviço que facilita a implantação e o gerenciamento de aplicativos na nuvem sem precisar gerenciar a infraestrutura subjacente.

- **AWS Lambda:**
  - Permite executar código sem precisar gerenciar servidores. O código é executado em resposta a eventos e pode ser escalado automaticamente.

- **Amazon RDS (Relational Database Service):**
  - Serviço gerenciado de banco de dados que facilita a configuração, operação e escalabilidade de bancos de dados relacionais na nuvem.

Exemplos de SaaS na AWS

- **AWS Trusted Advisor:**
  - Ferramenta online que **analisa o ambiente AWS e oferece orientações e recomendações em tempo real**, ajudando a seguir as melhores práticas da AWS.
  - Oferecido como parte do plano de suporte AWS, com recursos adicionais disponíveis para os planos Business Support e Enterprise Support.

- **AWS Shield:**
  - Serviço gerenciado de proteção contra ataques **DDoS (negação de serviço distribuída)**.
  - Proporciona mitigação automática e ativa para minimizar tempo de inatividade e latência dos aplicativos.
  - O AWS **Shield Advanced** oferece benefícios extras, com suporte especializado disponível para clientes com Enterprise ou Business Support.

- **Amazon Chime:**
  - Serviço de comunicação que permite **reuniões, bate-papo** e chamadas de negócios.
  - O pagamento é conforme o uso, sem taxas adiantadas, compromissos ou contratos de longo prazo.

Características do serviço e responsabilidade de segurança

Software como serviço (SaaS)

- O software é hospedado de maneira centralizada
- Licenciado em um modelo de assinatura ou pagamento conforme o uso.
- Os serviços normalmente são acessados por meio de um navegador da Web, um aplicativo móvel ou uma interface de programação de aplicativos (API)
- Os clientes não precisam gerenciar a infraestrutura que oferece suporte ao serviço

Exemplos de SaaS

AWS Trusted Advisor

AWS Shield

Amazon Chime

Controle de Acesso com AWS Identity and Access Management (IAM)

- O IAM permite gerenciar quem pode acessar os serviços de computação, armazenamento, banco de dados e aplicativos na Nuvem AWS.

- **Funcionalidades:**
  - Gerenciamento centralizado de permissões.
  - Controle granular de acesso por serviço e usuário.
  - Autenticação e autorização através de políticas específicas.

- **Exemplo:** Diferentes níveis de acesso para Amazon EC2, S3, DynamoDB, etc.

- **Benefício:** IAM oferece controle detalhado sobre o acesso aos recursos.

Controle de Acesso com AWS Identity and Access Management (IAM)

- **O AWS Identity and Access Management (AWS IAM)**
  - Gerenciar usuários
  - Permissões de usuário na AWS.
  - Gerenciar de forma centralizada os usuários,
  - As credenciais de segurança (como as chaves de acesso)
  - As permissões que controlam quais recursos da AWS os usuários podem acessar.

Identity and Access Management (IAM)

- **Principais Funcionalidades:**
  - **Controle Granular:** Especificação precisa de permissões por serviço e ação (ex. chamadas de API).
  - **Gerenciamento Centralizado:** Permite gerenciar o acesso a recursos de forma unificada.
  - **Políticas Customizadas:** Criação de permissões específicas para grupos e usuários.

Identity and Access Management (IAM)

- **Use o IAM para gerenciar o acesso aos recursos da AWS**
  - Um recurso é uma entidade em uma conta da AWS com a qual você pode trabalhar
  - **Exemplo de recursos:** uma instância do Amazon EC2 ou um bucket do Amazon S3

- **Exemplo:** controle quem pode encerrar instâncias do Amazon EC2

- **Defina direitos de acesso refinados**
  - **Quem** pode acessar o recurso
  - **Quais** recursos podem ser acessados e o que o usuário pode fazer com o recurso
  - **Como** os recursos podem ser acessados

IAM: componentes essenciais

- Uma ***pessoa*** ou ***aplicativo*** que pode se autenticar com uma conta da AWS.

Usuário do IAM

- Uma ***coleção de usuários do IAM*** que recebem autorização idêntica.

Grupo do IAM

- O documento que define ***quais recursos podem ser acessados*** e o nível de acesso a cada recurso.

Política do IAM

- Mecanismo útil para conceder um conjunto de permissões para fazer solicitações de serviço da AWS.

Função do IAM

Garantindo Segurança no Acesso aos Recursos da Nuvem AWS

- **Definição de Autenticação:**
  - Processo básico de segurança em que um usuário ou sistema deve comprovar sua identidade antes de obter acesso.

- **Acesso aos Recursos da AWS:**
  - Semelhante à autenticação em áreas restritas, o usuário deve apresentar credenciais para acessar os recursos da AWS.

Autenticar como um usuário do IAM para obter acesso

- Ao definir um usuário do IAM, você seleciona os tipos de acesso que o usuário tem permissão para usar.

- **Acesso programático**
  - Autentique usando:
    - ID da chave de acesso
    - Chave de acesso secreta
  - Fornece acesso à CLI e ao SDK da AWS

- **Acesso ao Console de Gerenciamento da AWS**
  - **Autentique usando:**
    - ID ou alias da conta com 12 dígitos
    - Nome de usuário do IAM
    - Senha do IAM

- Se ativada, a **Multi-Factor Authentication (MFA)** solicita um código de autenticação.

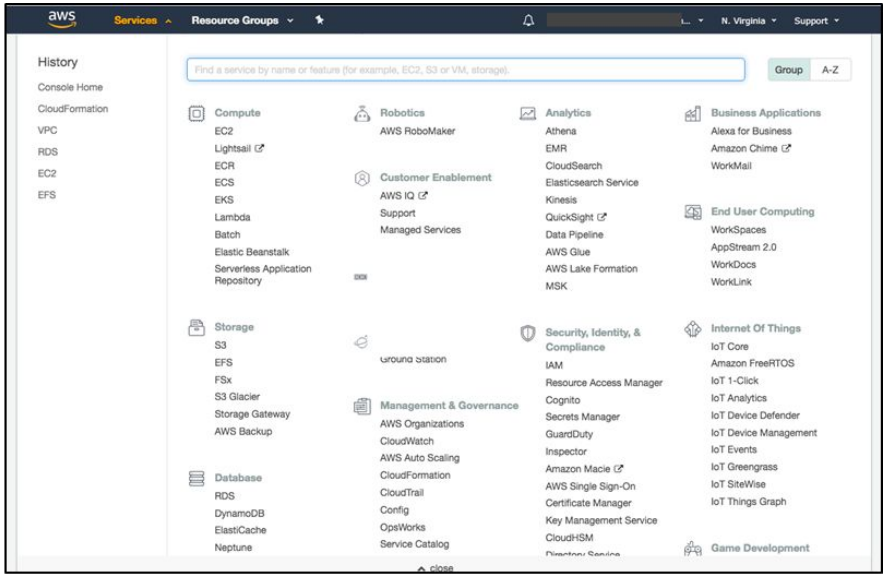
CLI da AWS

Ferramentas e SDKs da AWS

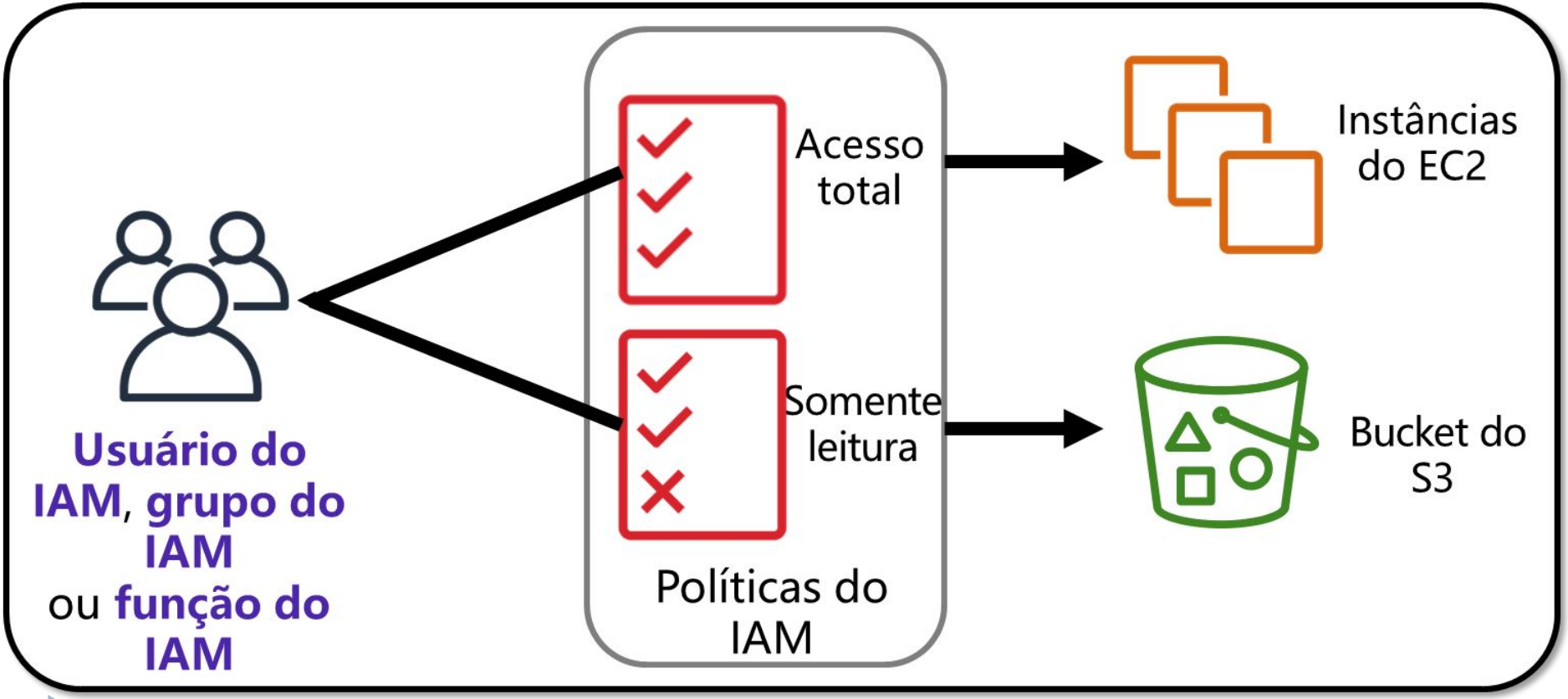
Console de Gerenciamento da AWS

MFA do IAM

- A MFA oferece maior segurança.
- Além do nome de usuário e da senha, a MFA requer um código de autenticação exclusivo para acessar os serviços da AWS.



Console de Gerenciamento da AWS


Usuário do IAM, grupo do IAM ou função do IAM
Acesso total
Somente leitura
Políticas do IAM
Instâncias do EC2
Bucket do S3

MUITO OBRIGADO!!!!!

Guto Muniz

augustomuniz@gmail.com